

Claims

What is claimed is:

- [c1] A method for re-encrypting encrypted data in a secure storage file system, comprising:
 - obtaining selected data to re-encrypt from the secure storage file system using a user data access record and the encrypted data;
 - decrypting the selected data using a symmetric key;
 - re-encrypting the selected data using a new symmetric key to obtain new encrypted data;
 - encrypting the new symmetric key using a public key to obtain a new encrypted symmetric key;
 - storing the new encrypted data and the new encrypted symmetric key if the public key is associated with a file system user having read permission; and
 - storing an encrypted hash data if the file system user has write permission.
- [c2] The method of claim 1, wherein the user data access record comprises at least one selected from the group consisting of a bitmap, a bitmap for each user, and a bitmap for each group of users.
- [c3] The method of claim 1, wherein the write permission comprises at least one sub-division.
- [c4] The method of claim 3, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.
- [c5] The method of claim 1, wherein the secure storage file system is implemented using a preloaded shared library.

- [c6] The method of claim 5, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.
- [c7] The method of claim 1, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.
- [c8] A method for re-encrypting a plurality of layer-encrypted data blocks in a secure storage file system, comprising:
 - obtaining at least one of the plurality of layer-encrypted data blocks from the secure storage file system to re-encrypt using a user data access record and the plurality of layer-encrypted data blocks;
 - decrypting the at least one of the plurality of layer-encrypted data blocks using a layer key; and
 - re-encrypting the at least one of the plurality of layer-encrypted data blocks using a new layer key to obtain a new layer-encrypted data block.
- [c9] The method of claim 8, wherein the user data access record comprising at least one selected from the group consisting of a bitmap, a bitmap for each user, and a bitmap for each group of users.
- [c10] The method of claim 8, wherein the at least one of the plurality of layer-encrypted data blocks comprises an encrypted symmetric key and encrypted data.
- [c11] The method of claim 8, wherein the at least one of the plurality of layer-encrypted data blocks comprises an encrypted symmetric key, an encrypted hash data, and encrypted data.
- [c12] The method of claim 8, wherein the layer key and the new layer key are provided by an authentication agent.

- [c13] A computer system generating a secure storage file system, comprising:
a processor;
a memory;
a storage device;
a computer display; and
software instructions stored in the memory for enabling the computer system
under control of the processor, to perform:
obtaining selected data to re-encrypt from the secure storage file system using a
user data access record and the encrypted data;
decrypting the selected data using a symmetric key;
re-encrypting the selected data using a new symmetric key to obtain new
encrypted data;
encrypting the new symmetric key using a public key to obtain a new encrypted
symmetric key;
storing the new encrypted data and the new encrypted symmetric key if the public
key is associated with a file system user having read permission; and
storing an encrypted hash data if the file system user has write permission.
- [c14] The computer system of claim 13, wherein the write permission comprises at least
one sub-division.
- [c15] The computer system of claim 15, wherein the sub-division is selected from a
group consisting of insert, append, truncate, and delete.
- [c16] The computer system of claim 13, wherein the secure storage file system is
implemented using a preloaded shared library.
- [c17] The computer system of claim 16, wherein the preloaded shared library translates
read/write/file name accesses into different read/write/file name accesses.

- [c18] The computer system of claim 13, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.
- [c19] The computer system of claim 13, wherein the user data access record comprises at least one selected from the group consisting of a bitmap, a bitmap for each user and a bitmap for each group of users.
- [c20] A secure storage system comprising:
a storage provider storing encrypted data, wherein re-encrypting the encrypted data comprises:
obtaining selected data to re-encrypt from the secure storage file system
executing on the storage provider using a user data access record and
the encrypted data based on receipt of a key re-encryption event;
decrypting the selected data using a symmetric key;
re-encrypting the selected data using a new symmetric key to obtain new
encrypted data;
encrypting the new symmetric key using a public key to obtain a new
encrypted symmetric key;
storing the new encrypted data and the new encrypted symmetric key if the
public key is associated with a file system user having read
permission; and
storing an encrypted hash data if the file system user has write permission;
and
a client device, wherein the client device comprises a client kernel for generating
the key re-encryption event and a client application using the encrypted
data.

- [c21] The system of claim 20, wherein the user data access record comprises at least one selected from the group consisting of a bitmap, a bitmap for each user, and a bitmap for each group of users.
- [c22] The system of claim 20, wherein the write permission comprises at least one sub-division.
- [c23] The system of claim 22, wherein the sub-division is selected from a group consisting of append, truncate, and delete.
- [c24] A secure storage system comprising:
a storage provider storing a plurality of layer-encrypted data blocks, wherein re-encrypting layer-encrypted data blocks comprises:
obtaining at least one of the plurality of layer-encrypted data blocks to re-encrypt from the secure storage file system executing on the storage provider using a user data access record and the plurality of layer-encrypted data blocks based on receipt of a key re-encryption event;
decrypting the at least one of the plurality of layer-encrypted data blocks using a layer key; and
re-encrypting the at least one of the plurality of layer-encrypted data blocks using a new layer key to obtain a new layer-encrypted data block;
and
a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the plurality of layer-encrypted data blocks.
- [c25] The system of claim 24, wherein the user data access record comprises at least one selected from the group consisting of a bitmap, a bitmap for each user, and a bitmap for each group of users.

- [c26] The system of claim 24, wherein of the plurality of at least one of the plurality of layer-encrypted data blocks comprise an encrypted symmetric key and encrypted data.
- [c27] The system of claim 24, wherein the at least one of the plurality of layer-encrypted data blocks comprise an encrypted symmetric key, an encrypted hash data, and encrypted data.
- [c28] The system of claim 24, wherein the layer key and the new layer key is provided by an authentication agent.
- [c29] An apparatus for re-encrypting a plurality of layer-encrypted data blocks in a secure storage file system, comprising:
means for obtaining at least of the plurality of one layer-encrypted data blocks to re-encrypt from a secure storage file system using a user data access record and the plurality layer-encrypted data blocks;
means for decrypting the at least one of the plurality of layer-encrypted data blocks using a layer key; and
means for re-encrypting the at least one of the plurality of layer-encrypted data blocks using a new layer key to obtain a new layer-encrypted data block.
- [c30] An apparatus for re-encrypting encrypted data in a secure storage file system, comprising:
means for obtaining selected data to re-encrypt from a secure storage file system using a user data access record and the encrypted data;
means for decrypting the selected data using a symmetric key;
means for re-encrypting the selected data using a new symmetric key to obtain new encrypted data;
means for encrypting the new symmetric key using a public key to obtain a new encrypted symmetric key;

means for storing the new encrypted data and the new encrypted symmetric key if
the public key is associated with a file system user having read permission;
and
means for storing an encrypted hash data if the file system user has write
permission.